UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/766,065	01/19/2001	Bradley Allen Bowlin	10006826-1	8299

7590 08/13/2004	EXAMINER
HEWLETT-PACKARD COMPANY	ZIA, MOSSADEQ

HEWLETT-PACKARD COMPANY
Inetllcutal Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 January 2001*.
2a)☐ This action is **FINAL**.　　2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
　　 closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.
　　 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-31* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
　　 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
　　 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
　　 a)☐ All　b)☐ Some * c)☐ None of:
　　　 1.☐ Certified copies of the priority documents have been received.
　　　 2.☐ Certified copies of the priority documents have been received in Application No. _____.
　　　 3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
　　　　　 application from the International Bureau (PCT Rule 17.2(a)).
　　 * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)
1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
　　 Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413)
　　 Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2.   Claims 1, 2, 5, 6-10, 14-16, 20-26, 29, 30, 31 are rejected under 35 U.S.C. 102(b) as

being anticipated by Patent No. 5,495,533, Linehan et al.

3.   Regarding claim 1, Linehan shows a method which enables a user to prevent

unauthorized access to files stored on a computer, comprising:

maintaining first database which identifies files (file header) stored on the computer to be

included in a safe zone (Linehan, col. col. 8, line 59-62);

maintaining a second database (access control list) which defines authorized accesses to

said files within said safe zone (Linehan, col. 7, line 59-60);

providing said computer with a filter (Personal Key client/server, Linehan, col. 7, line 6-

9);

upon a request for access to a file stored on said computer, utilizing said filter to access

said first database and determine whether said file is within said safe zone (file access, Linehan,

col. 7, line 54); and

if said file is determined to be within said safe zone, accessing said second database to determine whether said request to access said file has been authorized (Linehan, col. 7, line 57-60).

4.   Regarding claim 2, Linehan shows claim 1 above, and further show comprising, said request determined to be unauthorized, then denying access to said file, else granting access to said file (Linehan, col. 9, line 49-50).

5.   Regarding claim 5, Linehan shows claim 1 above, method as claim further comprising providing an interface through which said user can update said first database (Linehan, col. 8, line 4-6).

6.   Regarding claim 6, Linehan show claim 1, and further show comprising providing an interface through which said user can update said second database (Personal Key Client, Linehan, col. 9, line 59-61).

Regarding claim 7, Linehan show claim 1 above, and further show comprising encrypting said first database (Linehan, col. 8, line 64-65).

Regarding claim 8, Linehan show claim 1 above, and further encrypting said second database (Linehan, col. 8, line 64-65).

Regarding claim 9, Linehan show claim 1 above, wherein:

said first database is a distributed database (header, fig. 8), said distributed database comprising a file within each directory containing one or more of said files which were identified by said first database to be included within said safe zone (stored in the file's directory, Linehan, col. 8, line 50-54); and

said filter accessing (client) said first database comprises said filter accessing the files of said distributed database to verify whether said file for which access has been requested is within said safe zone (Linehan, col. 7, line 54-60).

7.   Regarding claim 10, Linehan shows claim 9 above, and further show comprising encrypting the files of said distributed database (Linehan, col. 8, line 64-65).

8.   Regarding claim 14, Linehan shows claim 1 above, and further show said filter is a part an operating system which is installed on said computer (computing system, Linehan, col. 4, line 61-62).

9.   Regarding claim 15, Linehan shows claim 1 above, and further show said filter is only activated by remote queries to said computer (distributed computing, Linehan, col. 4, line 29-32).

10.   Regarding claim 16, Linehan show apparatus which enables a user to prevent unauthorized access to files stored on a computer, comprising:

at least one computer readable storage media (Linehan, fig. 4, label 38);

and

computer readable program code stored on said at least one computer readable storage media, said computer readable program code comprising (computer, Linehan, fig. 4, label 36):

program code for maintaining a first database which identifies files stored on said computer to be included in a safe zone (Linehan, col. 7, line 39-42);

program code for maintaining second database which defines authorized accesses said files within said safe zone (Linehan, col. 7, line 59-60);

program code providing said computer with a filter (Personal Key client/server, Linehan, col. 7, line 6-9);

program code for utilizing said filter which enables a user prevent to files stored on

computer, access said first database and determine whether a file for which access has been

requested is within said safe zone (file access, Linehan, col. 7, line 54); and

program code for accessing said second database to determine whether said request to

access said file has been authorized if said file is determined to be within said safe zone.

(Linehan, col. 7, line 57-60).

11.   Regarding claim 20, Linehan shows claim 16 above, and further show comprising

program code for creating a first interface through which said user can update said first database

(Linehan, col. 8, line 4-6).

12.   Regarding claim 21, Linehan shows claim 16 above, and further comprising program

code for creating a second interface through which said user can update said second database

(Personal Key Client, Linehan, col. 9, line 59-61).

13.   Regarding claim 22, Linehan shows claim 16 above, and further show comprising

program code for encrypting said first database (Linehan, col. 8, line 64-65).

14.   Regarding claim 23, Linehan shows claim 16, and further show comprising program code

for encrypting said second database (Linehan, col. 8, line 64-65).

15.   Regarding 24, Linehan shows claim 16 above, and further show comprising program

code for creating distributed database (header, fig. 8), comprising a file within each directory

containing one or more of said files which were identified by said first database to be included in

said safe zone (stored in the file's directory, Linehan, col. 8, line 50-54), wherein said first

database comprises said distributed database, and wherein said filter accessing said first database

comprises said filter accessing the files of said distributed database to verify (message

authentication check) whether said file for which access has been requested is within said safe

zone (Linehan, col. 8, line 61-65).

16.   Regarding claim 25, Linehan shows claim 24, and further show comprising program code

for encrypting the files of said distributed database (Linehan, col. 8, line 64-65).

17.   Regarding claim 26, Linehan shows claim 16, and further show comprising program code

for attempting to determine whether said request for access was initiated by a Trojan process

(user) if said request for access is determined to have been made to a file within said zone, and if

said request for access is determined to be authorized (identifying is a user (a user is a subject

accessing an object) permitted to create or access data, Linehan, col. 4, line 63).

18.   Regarding claim 29, Linehan shows claim 16 above, and further show said filter is a part

of an operating system which is installed on said computer (computing system, Linehan, col. 4,

line 61-62).

19.   Regarding claim 30, Linehan shows claim 16 above, and further show said filter is only

activated by remote queries to said computer (distributed computing, Linehan, col. 4, line 29-32).

20.   Regarding claim 31, Linehan show an apparatus which enables user to prevent access

files stored on a computer, unauthorized comprising:

        means for identifying files stored on the computer to be included in a safe zone (Linehan,

col. 7, line 39-42);

        means for defining authorized accesses said files within said safe zone (access control

list, Linehan, col. 7, line 59-60);

        means for determining whether a file for which access has been requested is within said

safe zone (file access, Linehan, col. 7, line 54);

and

means for determining whether said request to access said file has been authorized (Linehan, col.

7, line 57-60).

Claim Rejections - 35 USC § 103

21.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

22.   Claims 11, 12, 13, 27, 28 are rejected under **35 U.S.C. 103(a)** as being unpatentable over

Patent No. 5,495,533, Linehan et al. in view of Patent No. 6,647,400, Moran.

23.   Regarding claim 11, Linehan shows claim 1 above, and show further comprising, if said

request for access is determined to have been made to a file within said safe zone, and if said

request is determined to be authorized (Linehan, col. 7, line 57-60), but fail to show attempting

to determine whether said request was initiated by a Trojan process.

However, Moran teach an intrusion detection system comprises a signature checking

mechanism configured to compute a signature of a file, compare it to a file signature previously

computed by the signature checking mechanism, and compare it to a file signature previously

computed by other than the signature checking mechanism (a determining step towards

identifying a Trojan, Moran, col. 4, line 9-16).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Linehan as per teaching of Moran to include the improved system and method for detecting computer intrusion (Moran, col. 3, line 21-22).

24.   Regarding claim 12, Linehan shows claim 11, and further show wherein attempting to determine whether said request was wherein attempting to initiated by a Trojan process comprises determining what application the request appears to be associated with, and also determining whether a timestamp which is associated with the request is consistent with one more timestamps associated with the application's install (Moran, col. 4, line 25-29).

25.   Regarding claim 13, Linehan shows claim 11 above, but fail to show further wherein attempting to determine whether said request was initiated by a Trojan process comprises determining whether a directory from which said request was launched is an appropriate location for the process making said request to be stored.

However, Moran teaches intrusion detection system comprises an analysis engine and a configuration discovery mechanism for locating system files on a host. The configuration discovery mechanism communicates the locations of these files to the analysis engine (Moran, col. 3, line 63-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Linehan and Trostle as per teaching of Moran to include the improved system and method for detecting computer intrusion (Moran, col. 3, line 21-22).

26.   Regarding claim 27, Linehan shows claim 26, but fail to further show the program code for attempting to determine whether said request was initiated by a Trojan process further comprises program code for determining what application said request appears to be associated

with and for determining whether a timestamp which is associated with said request is consistent with one or more timestamps associated with the application's install.

However, Moran teaches an intrusion detection system comprises a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file, filter out expected time steps, correlate them with other events, and assign a suspicion value to a record associated with an event (a request is an event, Moran, col. 4, line 25-29).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Linehan as per teaching of Moran to include the improved system and method for detecting computer intrusion (Moran, col. 3, line 21-22).

27.   Regarding claim 28, Linehan shows claim 26 above, but fail to further show the program code for attempting to determine whether said request was initiated by a Trojan process further comprises program code for determining whether a directory from which said request was launched is an appropriate location for the an process making said request to be stored.

However, Moran teach an intrusion detection system comprises a signature checking mechanism configured to compute a signature of a file, compare it to a file signature previously computed by the signature checking mechanism, and compare it to a file signature previously computed by other than the signature checking mechanism (a determining step towards identifying a Trojan, Moran, col. 4, line 9-16).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Linehan as per teaching of Moran to include the improved system and method for detecting computer intrusion (Moran, col. 3, line 21-22).

28.   Claims 3, 4, 17, 18, 19 are rejected under **35 U.S.C. 103(a)** as being unpatentable over

Patent No. 5,495,533, Linehan et al. in view of Patent No. 6,189,032, Susaki et al.

29.   Regarding claim 3, Linehan shows claim 2 above, but fail to show if access to said file is

denied, then subsequently prompting said user to confirm or reverse said decision to deny access.

        However, Susaki teaches displays (prompting) the identifier of a user who made the

service supply request, user authority level, and identifier of the service being the object of the

service supply request, which prompts to select a button to permit (confirm) or not permit (deny)

the approval request (Susaki, col. 11, line 57-62).

        Therefore, it would have been obvious to one of ordinary skill in the art at the time of the

invention to modify Linehan as per teaching of Susaki to provide a client-server system, a

server, and a client terminal, whereby, even if an approval and consent are required in case a user

of the client terminal receives a service that the server provides, the access to the foregoing

service by the concerned user can properly be controlled (Susaki, col. 2, line 48-52).

30.   Regarding claim 4, Linehan shows claim 3 above, but fail to show prompting said user to

confirm or reverse said decision to deny access comprises indicating to said user an identity of an

application that has requested access to said file.

        However, Susaki teaches displays (prompting) the identifier of a user who made the

service supply request, user authority level, and identifier of the service (application) being the

object of the service supply request, which prompts to select a button to permit (confirm) or not

permit (deny) the approval request (Susaki, col. 11, line 57-62).

        Therefore, it would have been obvious to one of ordinary skill in the art at the time of the

invention to modify Linehan as per teaching of Suzaki to provide a client-server system, a server,

and a client terminal, whereby, even if an approval and consent are required in case a user of the client terminal receives a service that the server provides, the access to the foregoing service by the concerned user can properly be controlled (Susaki, col. 2, line 48-52).

31.   Regarding claim 17, Linehan shows claim 16 above, further comprising program code for denying access to said file if said request is determined to be unauthorized, else for granting access to said file.

However, Susaki teaches displays the identifier of a user who made the service supply request, user authority level, and identifier of the service being the object of the service supply request, which prompts to select a button to permit (grant access) or not permit (deny) the approval request (Susaki, col. 11, line 57-62).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Linehan as per teaching of Susaki to provide a client-server system, a server, and a client terminal, whereby, even if an approval and consent are required in case a user of the client terminal receives a service that the server provides, the access to the foregoing service by the concerned user can properly be controlled (Susaki, col. 2, line 48-52).

32.   Regarding claim 18, Linehan shows claim 17 above, but fail to show comprising program code for prompting said user, if access to said file denied, to confirm or reverse said decision to deny access.

However, Susaki teaches displays (prompting) the identifier of a user who made the service supply request, user authority level, and identifier of the service (application) being the object of the service supply request, which prompts to select a button to permit (confirm) or not permit (deny) the approval request (Susaki, col. 11, line 57-62).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the

invention to modify Linehan as per teaching of Suzaki to provide a client-server system, a server,

and a client terminal, whereby, even if an approval and consent are required in case a user of the

client terminal receives a service that the server provides, the access to the foregoing service by

the concerned user can properly be controlled (Susaki, col. 2, line 48-52).
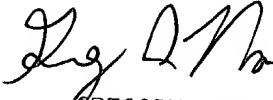
33.   Regarding claim 19, Linehan and Suzuki shows claim 18 above, and further show

comprising program code for indicating to said user an identity of an application that has

requested access to said file when said user is prompted to confirm or reverse said decision to

deny access (Susaki, col. 11, line 57-62).

Conclusion

34.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The

examiner can normally be reached on Monday-Friday between 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER

Mossadeq Zia
Examiner
Art Unit 2134

mz
8/5/04